VMware vShield Endpoint

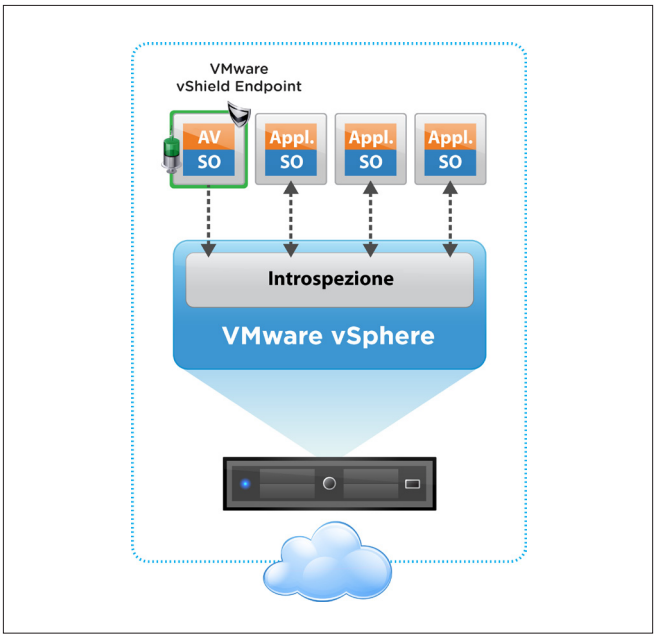
Prestazioni e sicurezza degli endpoint ottimizzate per i data center virtuali

IN BREVE

VMware vShield™ Endpoint rafforza la sicurezza delle macchine virtuali, ottimizzando enormemente le prestazioni degli endpoint in termini di protezione. vShield Endpoint demanda l'elaborazione delle attività antivirus e anti-malware ad appliance virtuali di sicurezza dedicate, distribuite dai partner VMware. La soluzione consente ai clienti di sfruttare gli investimenti esistenti e di gestire le policy antivirus e anti-malware per gli ambienti virtuali con le stesse interfacce di gestione utilizzate per la protezione degli ambienti fisici.

VANTAGGI PRINCIPALI

- Ottimizzazione dei rapporti di consolidamento e delle prestazioni mediante eliminazione degli agenti antivirus dalle macchine virtuali guest.
- Semplice implementazione e monitoraggio delle soluzioni antivirus e anti-malware negli ambienti VMware.
- Maggiore sicurezza mediante il consolidamento degli agenti software antivirus per la riduzione della superficie di attacco.
- Rispetto dei requisiti di conformità e auditing, con log dettagliati delle attività antivirus e anti-malware.



vShield Endpoint migliora le prestazioni e i rapporti di consolidamento delle soluzioni antivirus e anti-malware negli ambienti virtualizzati.

Presentazione di vShield Endpoint

vShield Endpoint rivoluziona il modo di concepire la protezione delle macchine virtuali guest da virus e malware. Questa soluzione ottimizza la protezione da virus e la sicurezza degli endpoint per gli ambienti VMware vSphere® e VMware View™.

vShield Endpoint migliora le prestazioni e le firme antivirus memorizzate demandando le attività di scansione dei virus dalle singole macchine virtuali a un'appliance virtuale di sicurezza dotata di motore di scansione virus. Questa architettura elimina il footprint degli agenti software nelle macchine virtuali guest, rende nuovamente disponibili le risorse di sistema, migliora le prestazioni ed elimina il rischio di un sovraccarico di lavoro causato dall'azione degli antivirus (sovraccarico delle risorse durante le scansioni pianificate e gli aggiornamenti della firme). Poiché l'appliance virtuale di sicurezza, a differenza della macchina virtuale guest, non passa in modalità offline, è in grado di effettuare l'aggiornamento costante delle firme antivirus, garantendo una protezione ininterrotta alle macchine virtuali sull'host. Inoltre, le nuove macchine virtuali (o le macchine virtuali esistenti passate in modalità offline) vengono protette immediatamente con le firme antivirus più aggiornate non appena tornano in modalità online.

vShield Endpoint ottimizza la protezione tramite un'unica appliance virtuale potenziata e immune da eventuali manomissioni (distribuita dai partner VMware) che ricorre alle solide funzionalità di introspezione dell'hypervisor presenti in vSphere, riducendo la vulnerabilità dei servizi antivirus e anti-malware.

Inoltre, vShield Endpoint offre ai partner VMware interfacce per l'implementazione della scansione dei file, della memoria e dei processi. Le aziende possono utilizzare simultaneamente più soluzioni di protezione; ad esempio, possono sfruttare la funzionalità di rilevamento dei dati sensibili di VMware vShield App con Data Security in un'appliance virtuale e al tempo stesso utilizzare una soluzione antivirus in un'altra appliance virtuale di sicurezza.

La conformità e il rispetto dei requisiti di auditing è dimostrabile tramite il log dettagliato delle attività generato dal servizio antivirus o anti-malware.

Gli amministratori possono gestire vShield Endpoint a livello centralizzato tramite la console di vShield Manager, inclusa nel pacchetto, che si integra perfettamente con VMware vCenter™ Server per semplificare la gestione unificata della sicurezza nei data center virtuali.

Funzionamento di vShield Endpoint

vShield Endpoint si integra direttamente in vSphere ed è costituito da tre componenti:

- Appliance virtuali di sicurezza rinforzate, distribuite dai partner VMware
- Thin agent per l'offload di eventi relativi alla sicurezza da parte delle macchine virtuali (incluso in VMware Tools)
- Modulo hypervisor VMware Endpoint ESX® per consentire la comunicazione tra i primi due componenti nel livello dell'hypervisor

Ad esempio, nel caso di una soluzione antivirus, vShield Endpoint esegue il monitoraggio degli eventi relativi al file della macchina virtuale e invia una notifica al motore antivirus, che procede alla scansione e a sua volta genera una risposta. La soluzione supporta le scansioni dei file all'accesso e on demand (pianificate) avviate dal motore antivirus nell'appliance virtuale di sicurezza.

Qualora sia necessario un intervento correttivo, gli amministratori possono specificare le azioni da intraprendere utilizzando gli strumenti di gestione antivirus e anti-malware esistenti; vShield Endpoint gestirà tutte le azioni di correzione nell'ambito delle macchine virtuali interessate.

Ambito di utilizzo di vShield Endpoint

La console di gestione, fornita dal partner VMware, viene utilizzata per configurare e controllare la soluzione software del partner ospitata nell'appliance virtuale di sicurezza. I partner VMware sono in grado di fornire un'interfaccia utente che offre un'esperienza della gestione (inclusa quella delle policy) analoga a quella della soluzione software ospitata su un'appliance di sicurezza fisica dedicata.

Agli amministratori dell'infrastruttura virtuale è richiesto un impegno notevolmente ridotto in quanto sulle macchine virtuali non sono installati agenti antivirus da gestire. Piuttosto, la console di gestione fornita dal partner viene utilizzata per gestire l'appliance virtuale di sicurezza. Questo approccio elimina la necessità di amministrare frequenti aggiornamenti per ogni macchine virtuale. Per quanto riguarda l'implementazione, VMware Tools include un thin agent e il modulo ESX che consente l'introspezione dell'hypervisor.

Gli amministratori dell'infrastruttura virtuale possono monitorare in modo semplice le implementazioni per determinare, ad esempio, il corretto funzionamento di una soluzione antivirus.

Funzionalità principali

Riassegnazione delle attività antivirus e anti-malware

- vShield Endpoint migliora le prestazioni mediante l'utilizzo del modulo ESX di vShield Endpoint che consente di demandare le attività antivirus a un'appliance virtuale di sicurezza in cui è attiva la scansione antivirus.
- Attività quali la scansione dei file, della memoria e dei processi vengono riassegnate dalle macchine virtuali a un'appliance virtuale di sicurezza tramite un agente thin client e il modulo ESX del partner.
- vShield Endpoint EPSEC gestisce la comunicazione tra le macchine virtuali e l'appliance virtuale di sicurezza ricorrendo all'introspezione nel livello dell'hypervisor.
- Il motore antivirus e i file delle firme vengono aggiornati solo sull'appliance virtuale incaricata della protezione, tuttavia le policy possono essere applicate a tutte le macchine virtuali dell'host vSphere.

Correzione

- vShield Endpoint applica le policy antivirus che determinano se sia necessaria l'eliminazione, la quarantena o una diversa gestione di un file dannoso.
- Il thin agent gestisce gli interventi correttivi sui file nell'ambito della macchina virtuale.

Integrazioni con i partner

- L'API EPSEC consente l'integrazione delle soluzioni antivirus dei partner VMware con vShield Endpoint tramite l'introspezione dell'attività dei file nell'hypervisor. Le funzioni antivirus di base sono supportate tramite questa API.

vShield Manager, gestione delle policy e automazione

- vShield Manager consente la distribuzione e la configurazione completa di vShield Endpoint.
- Le API REST (Representational State Transfer) consentono l'integrazione personalizzata delle funzionalità di vShield Endpoint nelle soluzioni utilizzate.
- Sono forniti report sul monitoraggio.
- vShield Manager può essere utilizzato come plug-in di vCenter.

Registrazione e auditing

- La registrazione degli eventi è basata sul formato standard syslog.

Versioni supportate

Per informazioni sulle versioni supportate degli ambienti vSphere, ESX e View, visitare http://vmware.com/it/products.

Prodotti correlati

La famiglia di soluzioni per la sicurezza vShield include inoltre VMware vShield Edge per la protezione perimetrale della rete; vShield App con Data Security per la protezione delle applicazioni dagli attacchi in rete e il rilevamento dei dati sensibili; vShield Manager e vShield Bundle, che include tutti i prodotti.

Ulteriori informazioni

Per informazioni o per acquistare i prodotti VMware, chiamare il numero (+39) 02 3041 2700, visitare il sito www.vmware.com/it/products oppure ricercare online un rivenditore autorizzato. Per informazioni dettagliate sulle specifiche di prodotto e i requisiti di sistema, consultare la Guida all'amministrazione di VMware vShield all'indirizzo http://www.vmware.com/pdf/vshield_41_admin.pdf.

Per ulteriori informazioni sui prodotti vShield, visitare http://vmware.com/it/products.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware Inc. - Via Spadolini, 5 - Edificio A - 20141 Milano - Tel. (+39) 02 3041 2700 Fax (+39) 02 3041 2701 www.vmware.com/it